UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of one vehicle registered to SALAZAR, a 2006 Toyota truck bearing California license plate, 87944C1(the "SUBJECT VEHICLE") as described in attachment A-3	)	Case No. 2:23-MJ-03993

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	receipt and distribution of child pornography
18 U.S.C. § 2252A(a)(5)(B)	possession of child pornography

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Natalie A. Bruford

Applicant's signature

FBI Special Agent Natalie A. Bruford

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Pedro V. Castillo, U.S. Magistrate Judge

Printed name and title

AUSA: Jeff Chemerinsky, ext. 6520

ATTACHMENT A-3

ITEM to BE SEARCHED:

A 2006 Toyota pick-up truck bearing California license plate #87944C1, the ("SUBJECT VEHICLE"), depicted below. The search of the aforementioned vehicle shall include any and all clothing and personal belongings, any digital devices, backpacks, wallets, briefcases, purses, and bags that are within the SUBJECT VEHICLE.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), namely:

a. Child pornography, as defined in Title 18, United States Code, Section 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in Title 18, United States Code, Section 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, in interstate commerce, including by computer, involving any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2)(B).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages,

that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that discuss, depict, or evidence any minor engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

f. Any and all records, documents, programs, applications, messages, notes, materials, or items that are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

g. Any and all records, documents, programs, applications, notes, materials, or items, including electronic mail and electronic messages, which discuss or otherwise may be related to the sex exploitation of children.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to KIK.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

j. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the SUBJECT PREMISES.

k. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of any digital device(s) found inside the SUBJECT PREMISES.

l. Any digital device, including but not limited to an Apple iPhone, which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

m. Any phone book, call log, or call records, digital or otherwise.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as

viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain

notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to SUBJECT PERSON believed to be a resident of the

SUBJECT PREMISES, and is the user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and/or is on SUBJECT PERSON's person, and which falls within the scope of the warrant, law enforcement personnel are authorized to: (1) direct the individual to depress the thumb- and/or fingerprints of the individual onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the individual with his/her eyes open (which law enforcement may direct) to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Natalie A. Bruford, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since July 2017. I am currently assigned to the Los Angeles Field Office where I have been working on the Violent Crimes Against Children Squad since September 2020. I am also assigned to the multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team. The SAFE Team is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under 18 U.S.C. § 2251, et seq. Through my work with the FBI, I have conducted and participated in numerous child pornography investigations and executions of search warrants and arrest warrants concerning individuals involved in the sexual exploitation of children and child pornography. I currently investigate criminal violations relating to the possession and production of child pornography in violation of 18 U.S.C. § 2252A.

2. I gained expertise in child exploitation investigations through formal training and on-the-job training with more experienced agents and received training and experience in interviewing and interrogating techniques, arrest procedures, search warrant applications, surveillance, and a variety of other investigative tools available to law enforcement officers. I addition, I received specialized training in the sexual

exploitation of children, observed and reviewed images of child pornography in many forms of media, including computer and digital media and participated in numerous interviews and debriefings of persons involved in the sexual exploitation of children.

3. Through both my training and experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children, and how people use the electronic devices and the Internet to commit crimes related to the sexual exploitation of children. As described in more detail below, I also have training and experience about the characteristics common to individuals with a sexual interest in children and images of children.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a warrant to search the premises located at 4020 Edenhurst Ave, Los Angeles, CA 90039 (the "SUBJECT PREMISES"), the person of RAUL SALAZAR JR (the "SALAZAR"), and one vehicle registered to SALAZAR, a 2006 Toyota truck bearing California license plate, 87944C1(the "SUBJECT VEHICLE"), more fully described below and in attachments A-1, A-2, and A-3, which are attached hereto and incorporated herein by reference.

5. The requested warrants seek authority to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) (collectively, the "SUBJECT OFFENSES"), more fully

described in Attachment B, which is attached herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

7. In December 2022, FBI Los Angeles received a lead from FBI Knoxville that their subject DEWAYNE PRICE, JR ("PRICE"), aka Kik username "drakious007," was in communication on August 26, 2022, with Kik username "imbackfaml" who disclosed to PRICE that he had sexual contact with all of their ex-girlfriend's daughters. Kik username "imbackfaml" was found to have asked PRICE if he had any videos, assumed to mean CSAM videos. PRICE transmitted at least one CSAM image to Kik username "imbackfaml," and Kik username "imbackfaml" distributed at least 3 CSAM images to PRICE.

8. A November 18, 2022, a Kik return revealed that the subscriber registered a Kik account associated with username "imbackfaml" on August 19, 2022, using a LGE LGL5676, registration email address herovee14@gmail.com and heroheroherov@gmail.com, and uploaded a profile image on August

20, 2022, using AT&T U-Verse IP 108.223.69.253 (SUBJECT PREMISES IP).

9. An AT&T return revealed the following subscriber for this IP address as MEGAN MURPHY, at 4020 Edenhurst Avenue Los Angeles, CA since February 8, 2016. A CLEAR search also revealed an individual named RAUL SALAZAR, to be associated with the residence.

10. FBI Los Angeles also obtained two CyberTiplines reported by MediaLab/Kik to the National Center for Missing and Exploited Children ("NCMEC") for two additional Kik accounts that had distributed CSAM from SUBJECT PREMISES IP. The first Kik account username "motherfirsst" distributed two CSAM files, in November and December 2020, with the registered email account of christina.michelle82@gmail.com. The second Kik account username "cashovaride" distributed nine CSAM files a total of fourteen times between January 2-4, 2022, with a registered email account of elephantalleyrs@gmail.com.

11. An FBI Los Angeles open-source search of the email address elephantalleyrs@gmail.com provided a Skype account with the same registered email to name of "Raul Salazar." On May 17, 2023, FBI Los Angeles received an administrative subpoena from Microsoft Corporation confirming the email address was registered to SALAZAR. The account was created on August 26, 2020, with the Skype IP address resolving to SUBJECT PREMISES IP.

12. Based on the investigation that followed, I have determined there is probable cause to believe that the SALAZAR

is the person utilizing the Kik username "imbackfaml." The Kik account that distributed CSAM from SUBJECT PREMISES IP is where SALAZAR currently resides.

13. FBI Los Angeles further determined that SUBJECT PREMISES IP was linked to two additional CyberTipline Reports from NCMEC indicating the distribution of CSAM. The Kik username "motherfirsst" uploaded two CSAM videos from SUBJECT PREMISES IP address in November and December of 2020. The Kik username "cashovaride" uploaded nine CSAM videos from SUBJECT PREMISES IP address in January of 2022. Additionally, the registered email account of the Kik username "cashovaride" is the same registered email address for a Skype account in the SALAZAR's true name.

14. Further investigation has linked SALAZAR to the SUBJECT VEHICLE that has been observed in the vicinity of the the SUBJECT PREMISES. Additionally, as described below, my training and experience provides reason to believe that SALAZAR will be preserving CSAM at the SUBJECT PREMISES, in the SUBJECT VEHICLE and/or on his person.

15. Accordingly, based on my training and experience, as well as my familiarity with this investigation, I believe probable cause exists that evidence of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE and on the person of SALAZAR.

IV. DEFINITION OF TERMS

16. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "computer" is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

c. The term "email" (electronic mail) is defined as the messages sent from one person to another via a computer. Email may also include files sent as attachments to or embedded within text messages. Email can also be sent automatically to a large number of addresses via a mailing list.

d. The term "Internet" is defined as the worldwide network of computers—a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of computer networks, online services, and single user components. In order to access the Internet, an individual computer or digital device user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

e. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

f. The term "IP Address" is defined as a unique number assigned to each computer or digital device directly connected to the Internet. Each computer or device connected to the Internet is assigned a unique IP address while it is connected (for example, 172.191.142.150). The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

g. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

h. The term "Cloud Storage" is defined as a network of online storage where data is saved in virtual storage that is hosted by third parties. The hosting companies operate large data centers, possibly across multiple servers. Cloud storage allows users to save files and data online and access their information from anywhere using any digital device with an Internet connection.

i. The terms "jpeg," "jpg," "gif," "bmp," and "art" are defined as graphic image files, namely, pictures.

j. The terms "mpeg," "mpg," "mov," "avi," "rm," and "wmv" are defined as video or movie files. To use these video files, one needs a personal computer or other digital device with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

k. The term "open source" is defined as software that includes a free license; in other words, it is freely available to everyone using the Internet.

l. The term "chat" means any kind of communication over the Internet that consists of the real-time transmission of messages between two or more users. Chat messages enable participants to respond quickly to one another and in a format that is similar to an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and e-mail.

V. BACKGROUND ON USE OF COMPUTERS, CHILD PORNOGRAPHY, AND FILE SHARING THROUGH MESSENGER APPLICATIONS

17. Based upon my training and experience in the investigation of child pornography and information related to me by other law enforcement officers involved in the investigation of child pornography offenses generally, I know the following information about the use of computers and child pornography:

18. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can scan these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

19. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, or from one digital or storage device to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer and digital device users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced, transported, and stored. For example, with the click of a button, someone trading images and videos containing child pornography with others through an online instant messaging application can be copied and put onto other digital devices or media storage devices such as external hard drives small enough to fit onto a keychain. Just as easily, these

files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

20. A growing phenomenon in mobile devices and smart phones is the use of applications, commonly known as "apps," to communicate between users. One such "app" is called KIK Messenger ("KIK"). "KIK" is a free chat application for mobile devices in which users can send text messages, photographs, videos, links, and other digital data to other users. KIK users can communicate directly with an individual or with multiple users in a group chat. When signing up for a KIK account, a user supplies an email address, a unique username, and a display name that is seen when chatting with other users. KIK is available for download through the iOS App Store and the Google Play store for most iOS and Samsung compatible phones and tablets. As more people are using their smart phones and mobile devices as their primary internet device, applications like KIK are used more frequently.

VI. STATEMENT OF PROBABLE CAUSE

A. Kik Username "imbackfaml" Distributes Child Pornography in August of 2022

21. In December of 2022, FBI Los Angeles received a lead from that their subject, PRICE, aka Kik username "drakious007", was in communication on August 26, 2022, with Kik username "imbackfaml," based on the return of a Kik search warrant. The following are excerpts from their chats that discuss their access to children:

drakious007: *Would you let me eat your daughter? (12:43:01 AM)*
imbackfaml: *Now when i think about it its hot*
Yes (12:43:26 AM)…

drakious007: *How many have you molested? (12:46:57 AM)*
imbackfaml: *All ex gf daughters*
3 (12:47:56 AM)…

drakious007: *I'd have to say my ex's 4 year old she couldn't tak so I played with her all the time (12:49:07 AM)*
How do you make your daughter lick your pussy
imbackfaml: *What would she say*
drakious007: *Nothing she couldn't ta k*
imbackfaml: *In the shower*
Ohh sorry
drakious007: *I mean do you grab her head and force her in your pussy?*

imbackfaml: *No im soft with het*

drakious007: *What do you tell her to get her to lick?*

imbackfaml: *Any of them like it*

drakious007: *Most was asleep they never knew*

imbackfaml: *Our special play time (12:51:30 AM)*

22. Kik username "imbackfaml" asked PRICE if he had any "pics or vids", assumed to mean CSAM images and videos. PRICE distributed at least one CSAM image to Kik username "imbackfaml", and Kik username "imbackfaml" distributes at least 3 CSAM images to PRICE. One is described as follows:

a. Image from 8/26/2022, at 1:05:11 AM: The image appears to depict a prepubescent female, approximate age of 8-11 years old. She is laying nude with her genitals exposed on a bed of sex toys and is inserting a dildo into her anus.

B. Identification of SUBJECT PREMISES

23. On November 18th, 2022, FBI Knoxville received a Kik return that revealed the account associated to the username "imbackfaml" was registered on August 19, 2022, using a LGE LGL5676. The registration email address was provided as herovee14@gmail.com and heroheroherov@gmail.com. A profile image was uploaded on August 20, 2022, using AT&T U-Verse IP 108.223.69.253.

24. FBI Knoxville was provided AT&T legal return that revealed the subscriber for IP 108.223.69.253 as Megan Murphy, at 4020 Edenhurst Avenue Los Angeles, CA (i.e., the SUBJECT

PREMISES), since February 8, 2016. A CLEAR search run by FBI Knoxville also revealed an individual named RAUL SALAZAR, to be associated with the residence.

25. On January 4, 2023, FBI Los Angeles searched the records of the California Department of Motor Vehicles (DMV) and confirmed that RAUL SALAZAR JR.'s California driver's license had a listed address of 4020 Edenhurst Ave. address as of July 24, 2019. This driver's license has an expiration date of October 26, 2024.

C. Kik usernames "motherfirsst" and "cashovaride" Distribute CSAM from SUBJECT PREMISES IP in 2020 and 2022.

26. On or around January 4, 2023, FBI Los Angeles ran SUBJECT PREMISES IP address through ICAC (Internet Crimes Against Children) Data System which provided two CyberTipline Reports. FBI Los Angeles obtained the two tips on or around January 5, 2023, from the National Center for Missing and Exploited Children ("NCMEC"). Both tips were reported to NCMEC by MediaLab/Kik.

a. The first Kik username account "motherfirsst" distributed two CSAM files, one on November 14, 2020, and the second on December 1, 2020, with the registered email account of christina.michelle82@gmail.com. An example of one the files is as follows:

i. Filename: 8e2e885a-fdcd-41c9a79597cff32f5524.mp4/ MD5:1af20725b9c13fa2380b9bccfe3515b5, Upload: 11-14-2020 23:37:09 UTC, IP Address: 108.223.69.253,

Description: An approximate 1 minute and 21 second video of a pubescent female, approximate age between 12-15 years old. She is face down on a bed with one hand tied behind her back in black cords. An adult nude male can be seen kneeling behind her continually inserting his erect penis into her vagina with her underwear/thong pushed to the side. A male voice in the room can be heard saying, "you can give it to her as hard as you want to man", "how does that feel Julie, good?", "she might be enjoying this a little too much", "this is just fucking tearing her up, its great".

b. The second Kik username account "cashovaride" distributed nine CSAM videos fourteen times between January 2-4, 2022, with the registered email account of elephantalleyrs@gmail.com. An example of one of the files is as follows:

i. Filename: 359de93f-b117-46ca-a8ee 6f64a543c7db.mp4/ MD5:cb1e8677009916073bcb0c897ff4e292, Upload: 01-03-2022 03:17:00 UTC, IP Address: 108.223.69.253, Description: The 59 second video appears to depict a prepubescent female between the approximate ages of 8-11 years old. The child is face down on a bed, and kneeling. The child wears a peach-colored top and is nude from the waste below. A nude male kneels behind her and can be seen continually inserting his erect penis into her vagina. When he pulls out the child puts her hands below her exposed vagina. An adult hand pulls her hand away to capture the cum in the child's vagina.

27. On or around January 10, 2023, FBI Los Angeles ran Kik username "cashovaride" against known FBI cases. It was discovered that "cashovaride" was in communication with the subject, Brent Walter Murie (MURIE), on a case based out of the FBI Richmond/Winchester Resident Agency. A Kik search warrant return revealed that "cashovaride" communicated with three Kik accounts attributed to MURIE. One Kik account, "macksfarm", provided viewable content.

28. The Kik search warrant return showed that "macksfarm" added "cashovaride" as a friend on January 5, 2022, at 3:55 pm. Kik username "cashovaride" was in receipt of eight videos from "macksfarm". The videos depicted apparent CSAM, primarily of prepubescent females with adult males. The CSAM videos were received between January 8, 2022 through January 26, 2022.

29. Kik username "cashovaride" distributed 4 videos to "macksfarm". The videos depict apparent CSAM of female victims. All files were distributed on January 10, 2022 from 9:50-9:52 AM. An example of one of the files is as follows:

a. Video File: cfd17c07-2f6a-427d-9bfb-047a7ae58b9d: A 1 minute and 29 second video of a nude prepubescent female between the approximate ages of 4-6 years old. She is laying on a beg with her legs spread so as to expose her vagina to the camera. An adult female pulls the child closer to the camera and inserts her pierced tongue and fingers into the vagina of the child.

D. SALAZAR Linked to Email Address elephantalleyrs@gmail.com

30. On or around January 4, 2023 FBI Los Angeles conducted an open source search of the email address elephantalleyrs@gmail.com and discovered a Skype account registered with the matching email in the name of RAUL SALAZAR. On May 17, 2023, FBI Los Angeles received an administrative subpoena from Microsoft Corporation confirming the email address was registered to SALAZAR. The account was created on August 26, 2020, with the Skype IP address resolving to SUBJECT PREMISES IP.

E. Observation of SALAZAR at SUBJECT PREMISES

31. On January 9, 2023, a physical surveillance was conducted in the vicinity of SUBJECT PREMISES. At approximately 7:12 AM, an adult male matching the height and weight of SALAZAR was observed exiting the vicinity of the SUBJECT PREMISES and walking towards the back parking lot of what appeared to be designated parking spots for residence of the apartment complex. A minute later a red pick-up truck was observed leaving the driveway of SUBJECT PREMISES. About two hours later the red pick-up truck, bearing California license plate 87944CI [registered to SALAZAR at 1207 8th St., San Fernando, California 91340] (i.e., the SUBJECT VEHICLE), was observed arriving and entering the driveway of the SUBJECT PREMISES. The adult male matching the height and weight of SALAZAR, was observed exiting

the SUBJECT VEHICLE, carrying a bag and seen walking into a unit within the vicinity of the SUBJECT PREMISES.

32. On May 23, 2023, a physical surveillance was conducted in the vicinity of SUBJECT PREMISES. At approximately 9:40 AM, an adult male matching the height, and weight of SALAZAR was observed exiting SUBJECT VEHICLE that was parked on road in front of SUBJECT PREMISES and enter SUBJECT PREMISES carrying a large blue/grey cooler. Agents additionally identified the male as SALAZAR based upon his photo from his California driver's license.

33. In sum, there is probable cause to believe that the individual utilizing the Kik username "imbackfaml" is SALAZAR. SALAZAR distributed CSAM, from SUBJCT PREMISE IP where he resides and drives the SUBJECT VEHICLE. This is principally based upon the following facts. First, the established Kik account utilizing username "imbackfaml" distributed CSAM from an SUBJCT PREMISE IP that is registered to the residence where he currently resides. Second, two additional CyberTipline Reports determined CSAM videos and images were uploaded from Kik username accounts, "motherfirsst" and "cashovaride" from SUBJECT PREMISE IP. Third, the email address associated to the Kik account for "cashovaride", was found to be the same email used for a Skype account in SALAZAR's true name.

34. Fourth, SALAZAR has been confirmed to reside at SUBJECT PREMISES based on observations of an individual matching SALAZAR's height and weight and driver's license photo driving to and from the SUBJECT PREMISES in SUBJECT VEHICLE.

35. Accordingly, based on the investigation as well as my training and experience, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE and on the person of SALAZAR. Moreover, as described in more detail in the following section, individuals involved in the SUBJECT OFFENSES tend to keep for long periods of time images and/or videos of child pornography. Individuals, such as the SALAZAR, are likely to possess these videos and images within their residence, on digital devices stored within their residence, in vehicles they operate, and on digital devices kept on their person. Keeping and maintaining these images and/or videos in their residence and on their person allows for quick and immediate access to the images and/or videos.

VII. TRAINING AND EXPERIENCE ON INDIVIDUALS WHO HAVE SEXUAL INTEREST IN CHILDREN

36. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that there are certain characteristics common to individuals with a sexual interest in children and images of children:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, in person, in

photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. This includes collecting images or videos traded with other like-minded individuals through online messaging applications such as KIK. Individuals who have a sexual interest in children or images of children oftentimes transfer, maintain, and store such materials, and use them for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess hard copies of child pornography, such as pictures, films, video tapes, magazines, negatives, photographs, and etcetera. As digital technology has developed, individuals with a sexual interest in children or images of children have become much more likely to maintain child pornography, including materials they may have obtained from, or shared with, other individuals through chat and file-sharing applications in digital or electronic format, stored either on digital devices or in remote storage locations on the Internet. Regardless of whether these individuals

collect their child pornography in hard copy or digital format, they may maintain their child pornography for a long period of time, even years. They usually maintain these collections in a safe, secure, and private environment, such as their homes, vehicles, or nearby, so they can view the child pornography at their leisure. These collections are typically highly valued.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/ collectors; may conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Additionally, individuals who receive or share child pornography with other online users often keep backups and copies of those materials on other digital or storage devices in their homes, cars, or other nearby locations.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

37. Based on my training and experience, as well as my conversations with digital forensics agents, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive,

deleted, or viewed via computer. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Because computer evidence is recoverable after long periods of time, and because there is probable cause to believe that persons at the SUBJECT PREMISES were once in possession of child pornography and likely obtained it from some as yet unidentified source, there is

probable cause to believe that evidence of activity related to the distribution, receipt, and possession and distribution of child pornography will be found at the SUBJECT PREMISES and on SALAZAR.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

38. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one

device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[1] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed

[1] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently

used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

39. As discussed herein, based on my training and experience I believe that digital devices will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID.

Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as

fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

40. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features

are considered to be a more secure way to protect a device's contents.

41. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

42. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

43. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to SALAZAR to be the user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1)

compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

44. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means

IX. CONCLUSION

45. Based on the foregoing, there is probable cause to believe that evidence, fruits and instrumentalities of the SUBJECT OFFENSES, as described above and in Attachment B, will be found in a search of the SUBJECT PREMISES, as described in Attachment A-1, SALAZAR, as described in Attachment A-2 of this affidavit, and the SUBJECT VEHICLE as described in Attachment A-3 of this affidavit.

NATALIE BRUFORD,
Special Agent,
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 8th day of August, 2023.

UNITED STATES MAGISTRATE JUDGE